Practitioner's Docket No. NAI1P092/01.050.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Jeffrey Green et al.

Application No.: 09/935,634 Group No.: 2142
Filed: August 24, 2001 Examiner: Lin, K.
For: SYSTEMS AND METHODS FOR CONVERTING INFECTED ELECTRONIC FILES TO A SAFE FORMAT

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF SUBSTITUTE APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal filed 02/03/2006, a substitute for the Appeal Brief filed 04/03/2006, and in response to the Notification of Non-Compliant Appeal Brief mailed on 01/23/2007.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. §1.17(c), the fee for filing the Appeal Brief has already been paid. However, the Commissioner is authorized to charge any fees that may be due to deposit account 50-1351 (NAI1P092).

4. EXTENSION OF TERM

Applicant believes that no extension of term in required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

ice to Addressee" (37 CFR 1.10) or facsimile transmission (37 CFR 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$0.00 (previously paid on April 3, 2006)
Extension of time	$0.00
Total Fee Due	$0.00

6. FEE PAYMENT

Applicant believes that only the above fees are due in connection with the filing of this paper because the appeal brief fee was paid with a previous submission. However, the Commissioner is authorized to charge any additional fees that may be due (e.g. for any reason including, but not limited to fee changes, etc.) to deposit account 50-1351 (Order No. NAI1P092).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P092).

/KEVINZILKA/

Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)	
	)	
Green et al.	)	Group Art Unit: 2142
	)	
Application No. 09/935,634	)	Examiner: Lin, Kelvin Y.
	)	
Filed: 08/24/2001	)	Date: February 23, 2007
	)	
For: SYSTEMS AND METHODS FOR CONVERTING INFECTED ELECTRONIC FILES TO A SAFE FORMAT	)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

SUBSTITUTE APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal filed 02/03/2006, a substitute for the Appeal Brief filed 04/03/2006, and in response to the Notification of Non-Compliant Appeal Brief mailed on 01/23/2007 (see attached). While appellant disagrees with the Examiner as to whether the alleged deficiencies exist in the original Appeal Brief, a Substitute Appeal Brief with appropriate edits is nevertheless submitted to expedite prosecution.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST

II RELATED APPEALS AND INTERFERENCES

III STATUS OF CLAIMS

IV STATUS OF AMENDMENTS

V SUMMARY OF CLAIMED SUBJECT MATTER

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, an appeal noted on 06/28/2006 in application serial number 09/935,635 may be, but is not necessarily, related.

Since no decision(s) has been rendered in such proceeding(s), no Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-10, 12-30 and 32-40

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-10, 12-30 and 32-40
3. Claims allowed: None
4. Claims rejected: 1-10, 12-30 and 32-40
5. Claims cancelled: 11 and 31

C. CLAIMS ON APPEAL

The claims on appeal are: 1-10, 12-30 and 32-40

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 1 and 2, a method carried out by a computer executing computer-readable program code comprises receiving a certain electronic file intended for delivery from a sender to an intended recipient (e.g. see item 202 of Figure 2, etc.) where the certain electronic file has a first file format with a first file extension and contains a computer virus. See, for example, paragraph 0017, et al. Prior to the certain electronic file being made available for viewing by the intended recipient (e.g. see item 206 of Figure 2, etc.), the certain electronic file is converted to a second file format having a second file extension that is different from the first file extension of the first file format (e.g. see item 204 of Figure 2, etc.) which prevents the computer virus from executing when the converted electronic file is opened by the intended recipient (e.g. see item 208 of Figure 2, etc.). See, for example, paragraph 0017, et al. The certain electronic file is converted in response to a determination that the certain electronic file represents at least the potential risk to the security of the computer system. See, for example, paragraph 0023, et al.

With respect to a summary of Claim 24, as shown in Figures 1 and 2, a method for implementing a security policy comprises determining whether an electronic file represents at least a potential risk to security of a computer system. See, for example, paragraph 0023, et al. Prior to making the electronic file available to an intended recipient of the electronic file (e.g. see item 206 of Figure 2, etc.), the electronic file is converted into a safe format having a safe file extension that ensures that a computer virus in the electronic file is unable to harm the computer system (e.g. see item 204 of Figure 2, etc.). The electronic file is converted in response to the determination that the electronic file represents at least the potential risk to the security of the computer system. See, for example, paragraph 0023, et al.

With respect to a summary of Claim 28, as shown in Figures 1 and 2, a computer-readable medium has instructions stored thereon, which, when executed by a computer, cause the computer to convert a certain electronic file, intended for delivery from a sender to an intended recipient (e.g. see item 200 of Figure 2, etc.), from a first file format having a first file extension to a second file format having a second file extension (e.g. see item 204 of Figure 2, etc.). See,

for example, paragraph 0017, et al. The converting is prior to the certain electronic file being made available for viewing by the intended recipient (e.g. see item 206 of Figure 2, etc.). The second file format with the second file extension is different from the first file format with the first file extension, and a computer virus in the certain electronic file is prevented from executing when the converted electronic file is opened by the intended recipient (e.g. see item 208 of Figure 2, etc.). See, for example, paragraph 0017, et al. The certain electronic file is converted in response to a determination that the certain electronic file represents at least the potential risk to the security of the computer system. See, for example, paragraph 0023, et al.

With respect to a summary of Claim 36, as shown in Figures 1 and 2, a computer has means for receiving a certain electronic file (e.g. see items 126a and 126b of Figure 1, and item 202 of Figure 2, etc.) intended for delivery from a sender to a intended recipient (e.g. see item 200 of Figure 2, etc.). The certain electronic file is a first file format with a first file extension and contains a computer virus. See, for example, paragraph 0017, et al. Further, prior to the certain electronic file being made available for viewing by the intended recipient (e.g. see item 206 of Figure 2, etc.), the computer includes means for converting the certain electronic file from the first file format with the first file extension to a second file format having a second file extension that is different from the first file format with the first file extension (e.g. see items 126a and 126b of Figure 1, and item 204 of Figure 2, etc.) which prevents the computer virus from executing when the converted electronic file is opened by the intended recipient (e.g. see item 208 of Figure 2, etc.). See, for example, paragraph 0017, et al. The certain electronic file is converted in response to a determination that the certain electronic file represents at least the potential risk to the security of the computer system. See, for example, paragraph 0012; paragraph 0017, lines 1-4, and paragraph 0023, et al.

Of course, the above citations merely provide examples of various claim language and possibly other features, and thus should not be construed as limiting in any manner.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1-10, 12-14, 16, 18-30, 32-33 and 35-40 under 35 U.S.C. 102(b) as being anticipated by Ji et al. (U.S. Patent No. 5,889,943).

Issue # 2: The Examiner has rejected Claims 15 and 34 under 35 U.S.C. 103(a) as being unpatentable over Ji et al. (U.S. Patent No. 5,889,943), in view of Chen (U.S. Patent No. 5,960,170).

Issue # 3: The Examiner has rejected Claim 17 under 35 U.S.C. 103(a) as being unpatentable over Ji et al. (U.S. Patent No. 5,889,943), in view of Chen (U.S. Patent No. 5,960,170), in further view of Maloney et al. (U.S. Patent No. 6,549,208).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1-10, 12-14, 16, 18-30, 32-33 and 35-40 under 35 U.S.C. 102(b) as being anticipated by Ji et al. (U.S. Patent No. 5,889,943).

Group #1: Claims 1-6, 8-10, 12, 13, 19-21, 23-30, 32-33 and 35-40

With respect to independent Claims 1, 24, 28 and 36, the Examiner has relied on the following excerpt from Ji to make a prior art showing of appellant's claimed "prior to the certain electronic file being made available for viewing by the intended recipient, converting the certain electronic file to a second file format having a second file extension that is different from the first file extension of the first file format and that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient" (see this or similar, but not identical, language in each of the foregoing claims).

> "...the mail sending module 281 may be used to forward messages or attachments to parties such as the sender and recipient of the treated message or the network administrator." (Col. 18, line 1-4)

In the Advisory Action dated 1/17/2006, the Examiner has responded to appellant's arguments by stating that Col. 8, lines 59-67 and Col. 9, lines 35-44 in "Ji clearly teaches checking the extension of the file name which including txt, bmd, pcx, and gif, that files are no likely to contain viruses, while exe, zip and com extension files are of the type that often contain viruses." The Examiner has concluded that "Ji discloses procedures (fig. 6B, step 610-612,or 610- 628) that prior to transferring the electronic file, there are steps to determine whether the file contains virus, then based on the user's configuration to rename the file." The Examiner has further argued that "the rename file not only can change the name, [but] it can also change the file extension" and that "[i]t is well known skill in the art of the computer field." Still yet, the Examiner as argued that "Ji teaches the option for users to specify in the configuration file to

prevent the virus from making damage before recipient open the file" and that thus "the virus-free extension is the target name."

First, appellant respectfully asserts that, in Ji, the file extension is only utilized to determine whether the file is of a type that can contain viruses, such that if the file is not of the type to contain viruses, then the file is transferred to the recipient (see Figure 6B). It appears that the Examiner has simply taken Ji's above mentioned limited use of file extensions, and has combined such limited use with Ji's teaching of renaming a file found to contain viruses, to meet appellant's claims.

Appellant respectfully asserts that, even if such combination of teachings are taken into account, simply nowhere does Ji even suggest "converting the certain electronic file to a second file format having a second file extension that is different from the first file extension of the first file format" (emphasis added), as appellant specifically claims. In fact, Ji teaches that after "the file is renamed and stored in a specified directory ... the user is notified of the new file name and directory path which can [be] used to manually request the file from the system administrator" (see Col. 9, lines 56-59). Clearly, such teaching does not even suggest that the file has been converted into a different format, in the manner specifically claimed by appellant.

Appellant again reiterates that renaming a file, as in Ji, simply means giving the file a new name. Appellant, on the other hand, claims converting the file to a different file format, and not merely giving the file a new name as taught in Ji. Specifically, nowhere in Ji is there any teaching of converting the file into a different format with a different extension (e.g. .TXT, etc.), as argued by the Examiner. Such extension, which is separate and different from a file name, is specifically indicative of a format thereof.

In addition, appellant reiterates that Ji also fails to disclose converting the file into a different file format "that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient." It seems the Examiner has simply inferred such a teaching from Ji's general disclosure of file formats that are not indicative of the file containing a virus. Again, the Examiner has failed to precisely show where appellant's specific language, when read in context, can be found. Appellant again respectfully asserts that such an inference is

unfounded. Specifically, in Ji, when a virus is found in a file, three options are provided, namely doing nothing and transferring the file, deleting the file without transferring it, or renaming the file and storing it (see Col. 9, lines 39-44 et al.). Thus, since Ji allows for a file to be transferred even after determining that the file is infected, etc. it is inappropriate to assume that renaming a file would inherently include converting the file into a different file format that specifically "prevents the computer virus from executing when the converted electronic file is opened by the intended recipient," as claimed by appellant. In other words, not only does Ji fail to meet appellant's claim language, it even *teaches away* from the same, as noted above.

As argued in the Amendment filed 06/3/05, it seems that the Examiner has relied on Ji's disclosure of sending mail messages that have been treated to meet appellant's specific claim language. Appellant respectfully asserts that Ji's "treated message" is simply a message that contained a virus and that was cleaned (see Col. 17, lines 34-52 for example). Thus, Ji merely teaches sending a message after it has been cleaned of any virus infection, which clearly does not meet "converting the certain electronic file to a second file format having a second file extension that is different from the first file extension of the first file format and that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient" in the manner claimed by appellant. Specifically, appellant claims changing the format of a file such that the virus contained in the file is prevented from executing, which clearly distinguishes the mere cleaning of the file as disclosed in Ji. It appears that the Examiner has simply failed to take into account the full weight of appellant's claims.

Still with respect to independent Claims 1, 24, 28 and 36, the Examiner has relied on the following excerpt from Ji to make a prior art showing of appellant's claimed technique "wherein it is determined whether the certain electronic file represents at least a potential risk to security of a computer system, said converting the certain electronic file being in response to a determination that the certain electronic file represents at least the potential risk to the security of the computer system" (see this or similar, but not identical, language in each of the foregoing claims).

> "...the mail scanning apparatus may then take corrective action 1225 regarding the infected message, by either removing the virus, sending a warning as part of the message, deleting the message or forwarding the message to a system administrator." (Col. 18, lines 47-51)

In the Advisory Action dated 1/17/2006, the Examiner has failed to respond to appellant's specific arguments. Appellant again respectfully asserts that Ji does not teach appellant's specific claim language for substantially the same reasons as argued above. Specifically, simply nowhere does Ji specifically disclose converting the file format, in the manner claimed by appellant.

As argued in the Amendment filed 06/3/05, appellant respectfully asserts that the corrective actions disclosed by Ji in the above cited excerpt relied on by the Examiner, including removing a virus, sending a warning with the message, deleting the message and forwarding the message, clearly fail to teach "converting the certain electronic file being in response to a determination that the certain electronic file represents the potential risk to the security of the computer system," as claimed by appellant. Specifically, appellant claims converting the file format, as described in the remaining claim language, whereas Ji merely cleans the infected file or leaves the file "as is."

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim (emphasis added).

This criterion has simply not been met by the Ji reference, for the reasons noted above.

Group #2: Claim 7

The Examiner has relied on Col. 12, lines 22-25 in Ji to make a prior art showing of appellant's claimed "converting occurring at a desktop computer of the intended recipient." Appellant respectfully asserts that such excerpt only discloses that "each of the encoded portions stored in its own file is individually decoded." Clearly, decoding encoded files does not even suggest "converting the certain electronic file to a second file format having a second file extension that

is different from the first file extension of the first file format and that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient" (emphasis added), as claimed. In addition, Ji expressly discloses that after the file is decoded, the file is checked for viruses and associated actions are taken, and then the transformed file is transmitted to the client (see Figure 8B and Col. 12, lines 56-59). Thus, in Ji, the file cannot be converted "at a desktop computer of the intended recipient," as appellant claims, since the file is transmitted after being decoded (emphasis added).

Again, appellant respectfully asserts that the Ji reference fails to meet all of appellant's claim language, as noted above.

Group #3: Claim 14

The Examiner has relied on the following excerpts from Ji to make a prior art showing of appellant's claimed "receiving a second electronic file intended for delivery from another sender to another intended recipient, the second electronic file having a third file format and containing another computer virus; and prior to the second electronic file being made available for viewing by the another intended recipient, converting the second electronic file to a fourth file format that is different from the third file format and that prevents the another computer virus from executing when the converted second electronic file is opened by the another intended recipient."

> "The messages may contain simple text, graphics files or complex executable files which, as indicated, may carry viruses." (Col. 13, lines 22-23)
>
> "...which may be of various types such as files generated by the electronic mail program 292 text editor, files generated by network application programs 296 such as word processing or spread sheet files, executable files, or any other object or item which may be conventionally attached to an electronic mail message or transferred to the client node 230 in an electronic mail system 200." (Col. 14, lines 32-38)

In the Advisory Action dated 1/17/2006, the Examiner has failed to respond to appellant's specific arguments. Thus, appellant substantially reiterates the arguments made in the Amendment dated 10/13/2005.

Specifically, in the Office Action dated 08/19/05, the Examiner has again relied on Ji's teaching of renaming a file (Col. 9, lines 1-44) to meet appellant's specific claim language. For substantially the same reasons as argued with respect to each of the independent claims above, appellant respectfully asserts that simply renaming a file does not meet "converting" in the context claimed by appellant.

As argued in the Amendment filed 06/3/05, appellant respectfully asserts that the above excerpts from Ji merely teach the type of messages that may carry viruses and the types of attachments that may be attached to such messages. Clearly, the above excerpts do not even suggest any sort of preventing virus execution in an electronic file, let alone in the specific manner claimed by appellant. Furthermore, nowhere in Ji is there any mention of "converting the second electronic file to a fourth file format that is different from the third file format and that prevents the another computer virus from executing when the converted second electronic file is opened by the another intended recipient," in the context claimed by appellant (emphasis added).

Again, appellant respectfully asserts that the Ji reference fails to meet all of appellant's claim language, as noted above.

Group #4: Claim 16

The Examiner has relied on Ji's disclosure of ".txt, .bmd, .pcx and .gif extension files" (Col. 8, line 67) and "encod[ing] binary data to ASCII data" (Col. 11, line 59) to make a prior art showing of appellant's claimed "second file format being at least one of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format."

Again, in the Advisory Action dated 1/17/2006, the Examiner has failed to respond to appellant's specific arguments. Thus, appellant substantially reiterates the arguments made in the Amendment dated 10/13/2005.

In particular, in the Office Action dated 08/19/05, the Examiner has argued that the types of files claimed by appellant are mentioned in Ji (Col. 8, line 67, Col. 9, lines 1-2). However, appellant notes that such excerpts merely disclose types of files likely to contain viruses and types of files not likely to contain viruses. In Ji, if the file is of a type that is likely to contain a virus, then the file is temporarily stored and analyzed to determine if it has a virus (see Col. 9, lines 14-20). Thus, the file formats determined in Ji only relate to determining whether to further analyze a file for viruses, and not to actually converting the file format, in the specific context claimed by appellant.

As argued in the Amendment filed 06/3/05, appellant respectfully asserts that simply disclosing types of files does rise to the level of specificity of appellant's claim language. In fact, the excerpts relied on by the Examiner are in the context of checking extensions of file names (Col. 8, line 66) and scanning messages for portions that have been encoded using uuencode (Col. 11, line 58). Clearly, neither of these contexts meet appellant's specific claim language, since appellant claims converting a first file format to a second file format, where the second file format is "at least on of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format," as claimed.

Again, appellant respectfully asserts that the Ji reference fails to meet all of appellant's claim language, as noted above.

Group #5: Claim 18

The Examiner has relied on Ji's disclosure of ".txt, .bmd, .pcx and .gif extension files" (Col. 8, line 67) and "encod[ing] binary data to ASCII data" (Col. 11, line 59) to make a prior art showing of appellant's claimed "second file format being the ACSII file format file." Again, in the Advisory Action dated 1/17/2006, the Examiner has failed to respond to appellant's specific arguments. Thus, appellant substantially reiterates the arguments made in the Amendment dated 10/13/2005.

In the Office Action dated 08/19/05, the Examiner has argued that the types of files claimed by appellant are mentioned in Ji (Col. 8, line 67, Col. 9, lines 1-2). However, appellant notes that such excerpts merely disclose types of files likely to contain viruses and types of files not likely to contain viruses. In Ji, if the file is of a type that is likely to contain a virus, then the file is temporarily stored and analyzed to determine if it has a virus (see Col. 9, lines 14-20). Thus, the file formats determined in Ji only relate to determining whether to further analyze a file for viruses, and not to actually converting the file format, in the specific context claimed by appellant.

As argued in the Amendment filed 06/3/05, appellant respectfully asserts that simply disclosing types of files does rise to the level of specificity of appellant's claim language. In fact, the excerpts relied on by the Examiner are in the context of checking extensions of file names (Col. 8, line 66) and scanning messages for portions that have been encoded using uuencode (Col. 11, line 58). Clearly, neither of these contexts meet appellant's specific claim language, since appellant claims converting a first file format to a second file format where "the second file format [is]... the ACSII file format file."

Again, appellant respectfully asserts that the Ji reference fails to meet all of appellant's claim language, as noted above.

Group #6: Claim 22

The Examiner has relied on the following excerpts from Ji to make a prior art showing of appellant's claimed "determining if the first file format is one of a word processing file format type and a graphics file format type, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it is determined that the certain file format is the word processing file format type, the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type."

"The analysis here is the same as step 618. In step 652, the output of the virus checking program is preferable echoed to the client task 72 by the FTP proxy server..." (Col. 10, lines 30-33)

"...the FTP proxy server 60 and SMTP proxy server 62 are preferably only included or installed in the memory 44 of the gateway nodes 32." (Col. 6, lines 50-53)

Yet again, in the Advisory Action dated 1/17/2006, the Examiner has failed to respond to appellant's specific arguments. Thus, appellant substantially reiterates the arguments made in the Amendment dated 10/13/2005.

In the Office Action dated 08/19/05, the Examiner has argued that the types of files claimed by appellant are mentioned in Ji. As argued with respect to the Amendment dated 06/3/05, appellant respectfully asserts that the above excerpts from Ji simply disclose an FTP proxy server that echoes the output of a virus checking program to a client task. Clearly, such a teaching has no relation to any sort of converting, in the manner claimed by appellant, and thus can in no way meet the same.

Again, appellant respectfully asserts that the Ji reference fails to meet all of appellant's claim language, as noted above.

Issue # 2:

The Examiner has rejected Claims 15 and 34 under 35 U.S.C. 103(a) as being unpatentable over Ji et al. (U.S. Patent No. 5,889,943), in view of Chen (U.S. Patent No. 5,960,170).

Group #1: Claims 15 and 34

Appellant respectfully asserts that the subject matter of such claims is deemed novel in view of the arguments made hereinabove.

Issue #4:

The Examiner has rejected Claim 17 under 35 U.S.C. 103(a) as being unpatentable over Ji et al. (U.S. Patent No. 5,889,943), in view of Chen (U.S. Patent No. 5,960,170), in further view of Maloney et al. (U.S. Patent No. 6,549,208).

Group #1: Claim 17

The Examiner has relied on Col. 10, lines 35-40 in Maloney to make a prior art showing of appellant's claimed "second file format being the HTML file format without scripts." Appellant respectfully asserts that such excerpt only teaches a JPG or GIF image "is not displayable in the recorded format" and that the "graphic extraction tool converts the reassembled HTTP session file containing JPG and GIF data and creates a new log file containing the names and images." Thus, in Maloney, the HTTP session file itself is converted, which clearly does not meet appellant's "second file format being the HTML file format without scripts," as claimed, when read in context.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A method carried out by a computer when executing computer-readable program code, the method comprising:

receiving a certain electronic file intended for delivery from a sender to an intended recipient, the certain electronic file having a first file format having a first file extension and containing a computer virus; and

prior to the certain electronic file being made available for viewing by the intended recipient, converting the certain electronic file to a second file format having a second file extension that is different from the first file extension of the first file format and that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient;

wherein it is determined whether the certain electronic file represents at least a potential risk to security of a computer system, said converting the certain electronic file being in response to a determination that the certain electronic file represents at least the potential risk to the security of the computer system.

2. (Original) The method of claim 1, the certain electronic file being an attachment to an electronic mail sent over a network.

3. (Original) The method of claim 2, the network including the internet.

4. (Original) The method of claim 1, said receiving occurring at a desktop computer of the intended recipient.

5. (Original) The method of claim 1, said receiving occurring at a server computer.

6. (Original) The method of claim 1, said receiving occurring at a gateway computer.

7. (Original) The method of claim 1, said converting occurring at a desktop computer of the intended recipient.

8. (Original) The method of claim 1, said converting occurring at a server computer.

9. (Original) The method of claim 1, said converting occurring at a gateway computer.

10. (Original) The method of claim 1, said converting occurring prior to the intended recipient receiving the certain electronic file.

11. (Cancelled)

12. (Previously Presented) The method of claim 1, said determining whether the certain electronic file represents the potential risk comprising:

determining if the certain electronic file contains the computer virus.

13. (Previously Presented) The method of claim 1, said determining whether the certain electronic file represents the potential risk comprising:

conducting a heuristic scan of the certain electronic file.

14. (Original) The method of claim 1, the certain electronic file being a first electronic file, further comprising:

receiving a second electronic file intended for delivery from another sender to another intended recipient, the second electronic file having a third file format and containing another computer virus; and

prior to the second electronic file being made available for viewing by the another intended recipient, converting the second electronic file to a fourth file format that is different from the third file format and that prevents the another computer virus from executing when the converted second electronic file is opened by the another intended recipient.

15. (Original) The method of claim 1, the computer virus including a macro virus.

16. (Original) The method of claim 1, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format.

17. (Original) The method of claim 16, the second file format being the HTML file format without scripts.

18. (Original) The method of claim 16, the second file format being the ACSII file format file.

19. (Original) The method of claim 16, the second file format being the TXT file format.

20. (Original) The method of claim 1, the second file format being a file format having text without scripts.

21. (Original) The method of claim 1, the certain electronic file being at least one of a word processing file, a spreadsheet file, a database file, a graphics file, a presentation file, a compressed file, and a binary executable file.

22. (Original) The method of claim 1, further comprising:

determining if the first file format is one of a word processing file format type and a graphics file format type, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it is determined that the certain file format is the word processing file format type, the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type.

23. (Original) The method of claim 1, the certain electronic file being an electronic file received by at least one of a RTP transfer or a HTTP transfer protocol.

24. (Previously Presented) A method for implementing a security policy, the method comprising:

determining whether an electronic file represents at least a potential risk to security of a computer system; and

prior to making the electronic file available to an intended recipient of the electronic file, converting the electronic file into a safe format having a safe file extension that ensures that a computer virus in the electronic file is unable to harm the computer system;

said converting the electronic file being in response to the determination that the electronic file represents at least the potential risk to the security of the computer system.

25. (Original) The method of 24, said determining comprising:

determining whether the electronic file has a file extension indicative of a file type that supports a potential computer virus.

26. (Original) The method of 24, said determining comprising:

detecting whether the electronic file contains the computer virus.

27. (Original) The method of 24, said determining comprising:

determining whether content of the electronic file reflects a potential computer virus.

28. (Previously Presented) A computer-readable medium having instructions stored thereon, the instructions when executed by a computer cause the computer to:

convert a certain electronic file, intended for delivery from a sender to an intended recipient, from a first file format having a first file extension to a second file format having a second file extension, said converting being prior to the certain electronic file being made available for viewing by the intended recipient, the second file format with the second file extension being different from the first file format with the first file extension and preventing a computer virus in the certain electronic file from executing when the converted electronic file is opened by the intended recipient;

wherein it is determined whether the certain electronic file represents at least a potential risk to security of a computer system, said converting the certain electronic file being in response

to a determination that the certain electronic file represents at least the potential risk to the security of the computer system.

29. (Original) The computer-readable medium of claim 28, the certain electronic file being an attachment to an electronic mail sent over a network.

30. (Original) The computer-readable medium of claim 28, the instructions when executed by the computer cause the computer to convert the certain electronic file from the first file format to the second file format prior to the intended recipient receiving the certain electronic file.

31. (Cancelled)

32. (Previously Presented) The computer-readable medium of claim 28 said determining whether the certain electronic file represents the potential risk comprising:

determining if the certain electronic file contains the computer virus

33. (Original) The computer-readable medium of claim 28, the instructions when executed by the computer further cause the computer to:

determine if the first file format is one of a word processing format type and a graphics format type, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it is determined that the first file format is the word processing file format type, the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type.

34. (Original) The computer-readable medium of claim 28, the computer virus being a macro virus.

35. (Original) The computer-readable medium of claim 28, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format.

36. (Previously Presented) An apparatus comprising:

a computer having means for receiving a certain electronic file intended for delivery from a sender to a intended recipient, the certain electronic file having a first file format having a first file extension and containing a computer virus, the computer further including means for converting, prior to the certain electronic file being made available for viewing by the intended recipient, the certain electronic file from the first file format with the first file extension to a second file format having a second file extension that is different from the first file format with the first file extension and that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient;

wherein it is determined whether the certain electronic file represents at least a potential risk to security of a computer system, said converting the certain electronic file being in response to a determination that the certain electronic file represents at least the potential risk to the security of the computer system.

37. (Original) The apparatus of claim 36, said computer being a desktop computer of the intended recipient.

38. (Original) The apparatus of claim 36, said computer being a server computer of a local area network.

39. (Original) The apparatus of claim 36, said computer being a gateway computer.

40. (Previously Presented) The method as recited in claim 1, wherein the first format is selected from the group consisting of: a word processing file, a spreadsheet file, a database file, a graphics file, a presentation file, a compressed file, and a binary executable file; and is converted to the second format which is selected from the group consisting of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

Since no decision(s) has been rendered in such proceeding(s), no material is included in this Related Proceedings Appendix.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P092).

Respectfully submitted,

By: /KEVINZILKA/ Date: February 23, 2007

Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/935,634	08/24/2001	Jeffrey Green	NAII P092/01.050.01	1385

28875 7590 01/23/2007

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
ART UNIT	PAPER NUMBER

DATE MAILED: 01/23/2007

Please find below and/or attached an Office communication concerning this application or proceeding.

Notification of Non-Compliant Appeal Brief (37 CFR 41.37)	Application No.	Applicant(s)	
	09/935,634	GREEN ET AL.	
	Examiner	Art Unit	
	Kelvin Lin	2142	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The Appeal Brief filed on _____ is defective for failure to comply with one or more provisions of 37 CFR 41.37.

To avoid dismissal of the appeal, applicant must file anamended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer. **EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.**

1. ☐ The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.

2. ☐ The brief does not contain a statement of the status of all claims, (e.g., rejected, allowed, withdrawn, objected to, canceled), or does not identify the appealed claims (37 CFR 41.37(c)(1)(iii)).

3. ☐ At least one amendment has been filed subsequent to the final rejection, and the brief does not contain a statement of the status of each such amendment (37 CFR 41.37(c)(1)(iv)).

4. ☒ (a) The brief does not contain a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings, if any, by reference characters; and/or (b) the brief fails to: (1) identify, for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function under 35 U.S.C. 112, sixth paragraph, and/or (2) set forth the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification by page and line number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(v)).

5. ☐ The brief does not contain a concise statement of each ground of rejection presented for review (37 CFR 41.37(c)(1)(vi))

6. ☐ The brief does not present an argument under a separate heading for each ground of rejection on appeal (37 CFR 41.37(c)(1)(vii)).

7. ☐ The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(viii)).

8. ☐ The brief does not contain copies of the evidence submitted under 37 CFR 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner **and relied upon by appellant in the appeal**, along with a statement setting forth where in the record that evidence was entered by the examiner, as an appendix thereto (37 CFR 41.37(c)(1)(ix)).

9. ☐ The brief does not contain copies of the decisions rendered by a court or the Board in the proceeding identified in the Related Appeals and Interferences section of the brief as an appendix thereto (37 CFR 41.37(c)(1)(x)).

10. ☐ Other (including any explanation in support of the above items):

With regard to claim 36, which includes means plus function limitations, the applicants have not identified the structure as corresponding to the claimed function. For example, with respect to the means for receiving an electronic file, the Applicants have pointed to item 202 of Figure 2. Likewise, with respect to the means for converting, the Applicants have pointed to item 204 of Figure 2. These items are merely a boxes in a flowchart that performs the function. The specification does not describe what structures other than the computer of claim 36 performing these functions. The computer cannot be the structure for performing these functions since it is the computer that is being claimed.

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER